					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P06					Titlu tad-dokument: **Politika tal-Ġestjoni tar-Riskju**							
Verżjoni: 1.0		Data tad-dħul fis-seħħ: 01.01.2025			Sid tad-dokument:							
X	Politika		Standard		Proċedura		Formola		Reġistru		Oħra	

Storja tar-reviżjonijiet				
Numru tar-reviżjoni	**Data tar-reviżjoni**	**Bidliet**	**Ivrevedut minn**	**Sid tal-proċess**

Approvazzjonijiet			
Isem	**Pożizzjoni**	**Data**	**Firma**

Allinjata ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżoli 6.1, 8.32, 10	Qalba tal-identifikazzjoni u l-ġestjoni tar-riskju, integrazzjoni fil-ġestjoni tat-tibdil, titjib kontinwu
ISO/IEC 27005:2024	Metodoloġija sħiħa taċ-ċiklu tal-ħajja tar-riskju	Proċess sħiħ tal-ġestjoni tar-riskju f’konformità mal-istandard
ISO 31000:2018	Prinċipji u qafas tal-ġestjoni tar-riskju	Prinċipji tal-ġestjoni tar-riskju adottati fil-qafas
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Gwida u struttura għall-valutazzjonijiet tar-riskju, governanza tar-riskju fuq livelli differenti
GDPR tal-UE	Artikoli 24, 25, 32	Proċessi u kontrolli tar-riskju għall-protezzjoni tad-data
Direttiva NIS2 tal-UE	Artikolu 21(2)(a–d)	Obbligi ta’ valutazzjoni tar-riskju u tas-sigurtà
DORA tal-UE	Artikoli 5, 6	Ġestjoni tar-riskju tal-ICT u reżiljenza operattiva
COBIT 2019	APO12, MEA	Struttura u sorveljanza tal-ġestjoni tar-riskju

1. Għan

1.1 Din il-politika tistabbilixxi qafas unifikat u formalizzat għall-identifikazzjoni, l-analiżi, il-valutazzjoni, it-trattament, il-monitoraġġ u r-rieżami tar-riskji tas-sigurtà tal-informazzjoni fl-organizzazzjoni kollha.

1.2 Tiżgura l-applikazzjoni konsistenti ta’ prinċipji bbażati fuq ir-riskju li jipproteġu l-Kunfidenzjalità, l-Integrità u d-Disponibbiltà (CIA) tal-assi tal-informazzjoni, f’konformità mal-Klawżola 6.1 ta’ ISO/IEC 27001:2022 u ma’ ISO 31000:2018.

1.3 Din il-politika tintegra l-ġestjoni tar-riskju tas-sigurtà tal-informazzjoni fil-proċessi tat-teħid tad-deċiżjonijiet tal-organizzazzjoni sabiex jintlaħqu l-objettivi strateġiċi interni u r-rekwiżiti regolatorji esterni.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-unitajiet organizzattivi kollha, għall-proċessi tan-negozju, għas-sistemi, għall-persunal u għall-arranġamenti ma’ partijiet terzi involuti fl-immaniġġjar, l-iżvilupp, il-ħażna jew il-ġestjoni tal-assi tal-informazzjoni.

2.2 Il-kamp ta’ applikazzjoni jestendi għal assi fiżiċi, diġitali u assi ospitati fil-cloud, inklużi data strutturata u data mhux strutturata, applikazzjonijiet, infrastruttura, netwerks u servizzi.

2.3 Din il-politika tkopri r-riskji tas-sigurtà tal-informazzjoni fil-livelli strateġiċi, operattivi, tal-proġetti u tekniċi, u hija obbligatorja għall-impjegati, il-kuntratturi u l-forniturі tas-servizzi kollha involuti f’attivitajiet tal-ISMS.

2.4 Il-ġestjoni tar-riskju għandha tiġi applikata għax-xenarji li ġejjin:

2.4.1 Implimentazzjoni ta’ proġett jew sistema ġdida

2.4.1.1 Bidliet sinifikanti (eż. arkitettura, sjieda, proċessi)

2.4.1.2 Integrazzjoni ta’ fornituri u ftehimiet ma’ partijiet terzi

2.4.1.3 Rispons għall-inċidenti u rieżamijiet ta’ wara l-inċident

2.4.1.4 Rieżamijiet perjodiċi tar-riskju organizzattiv jew awditi

3. Objettivi

3.1 Jiġi stabbilit u operazzjonalizzat proċess tal-ġestjoni tar-riskju ripetibbli fl-organizzazzjoni kollha, ibbażat fuq il-metodoloġiji ta’ ISO/IEC 27005 u ISO 31000.

3.2 Jiġi żgurat li r-riskji jiġu identifikati, analizzati, ivvalutati u ttrattati permezz ta’ metodi strutturati u traċċabbli, inklużi l-assenjazzjoni tas-sjieda tar-riskju u r-rabtiet mal-kontrolli.

3.3 Jinżammu Reġistru tar-Riskji ċentralizzat u taħt kontroll tal-verżjoni, kif ukoll Pjan ta’ Trattament tar-Riskju, li jirriflettu l-istat attwali tar-riskju, il-kopertura tal-kontrolli u l-progress tal-mitigazzjoni.

3.4 Jiġi żgurat li d-deċiżjonijiet dwar ir-riskju jkunu allinjati mal-Aptit għar-Riskju u mal-limiti ta’ tolleranza dokumentati, u li jippermettu deċiżjonijiet ta’ governanza infurmati dwar l-aċċettazzjoni, il-mitigazzjoni, it-trasferiment jew l-evitar tar-riskju.

3.5 Jiġu mmonitorjati kontinwament ix-xejriet tar-riskju u tiġi żgurata l-effettività tat-trattamenti tar-riskju, filwaqt li jkunu possibbli aġġustamenti proattivi abbażi tal-evoluzzjoni tat-theddid jew ta’ bidliet fin-negozju.

4. Rwoli u responsabbiltajiet

4.1 Maniġment Eżekuttiv / Bord tad-Diretturi

4.1.1 Japprova l-qafas tal-ġestjoni tar-riskju u jiddefinixxi l-Aptit għar-Riskju aċċettabbli u l-limiti ta’ tolleranza.

4.1.2 Jawtorizza strateġiji ta’ trattament tar-riskju għal riskji residwi li jaqbżu t-tolleranza.

4.1.3 Jalloka r-riżorsi u s-sorveljanza meħtieġa għat-tħaddim effettiv tal-programm tal-ġestjoni tar-riskju.

4.2 Maniġer tal-ISMS / Uffiċjal tar-Riskju

4.2.1 Huwa s-sid ta’ din il-politika u jżommha allinjata mal-istandards ISO/IEC 27001 u 27005.

4.2.2 Imexxi l-proċess tal-valutazzjoni tar-riskju fil-livell tal-intrapriża u jżomm ir-Reġistru tar-Riskji u l-Pjan ta’ Trattament tar-Riskju.

4.2.3 Jiżgura rieżamijiet perjodiċi u l-eskalazzjoni tar-riskji ewlenin lit-tmexxija eżekuttiva jew lill-Kumitat ta’ Tmexxija tal-ISMS.

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Rekwiżiti ta’ rieżami u aġġornament

9.1 Din il-politika u l-qafas assoċjat magħha għandhom jiġu rieżaminati kull sena, jew:

9.1.1 Wara avveniment ewlieni ta’ riskju jew inċident tas-sigurtà tal-informazzjoni

9.1.2 Wara bidla organizzattiva jew teknika sinifikanti

9.1.3 Bi tweġiba għal sejbiet tal-awditjar jew rekwiżiti regolatorji ġodda

9.2 Il-Maniġer tal-ISMS, l-Uffiċjal tar-Riskju u t-tim tal-Konformità huma responsabbli b’mod konġunt għal:

9.2.1 It-tnedija taċ-ċiklu tar-rieżami

9.2.2 Il-ġbir ta’ kontributi mill-unitajiet tan-negozju

9.2.3 Ir-reviżjoni tal-proċeduri u tal-limiti kif meħtieġ

9.3 Ir-reviżjonijiet kollha għandhom ikunu:

9.3.1 Taħt kontroll tal-verżjoni u rreġistrati

9.3.2 Approvati mill-Maniġment Eżekuttiv

9.3.3 Ikkomunikati lill-partijiet interessati

9.3.4 Miżmuma fir-repożitorju tal-awditjar għal minimu ta' 5 snin

10. Politiki relatati u rabtiet

10.1 Din il-politika hija interdipendenti mal-politiki li ġejjin tas-sigurtà tal-informazzjoni:

10.1.1 P1 – Politika tas-Sigurtà tal-Informazzjoni: Tistabbilixxi l-mudell ġenerali ta' governanza tas-sigurtà li taħtu topera din il-politika dwar ir-riskju.

10.1.2 P2 – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tiddefinixxi s-sidien responsabbli u l-livelli ta' governanza msemmija fil-matriċi tal-eskalazzjoni tar-riskju.

10.1.3 P5 – Politika tal-Ġestjoni tat-Tibdil: Tniedi rivalutazzjoni tar-riskju għal bidliet fl-infrastruttura u fl-organizzazzjoni.

10.1.4 P13 – Politika tal-Klassifikazzjoni u t-Tikkettar tad-Data: Tappoġġa l-valutazzjoni tal-impatt waqt l-identifikazzjoni tar-riskju.

10.1.5 P33 – Politika tal-Monitoraġġ tal-Awditjar u l-Konformità: Tikkonferma l-konformità ma' din il-politika, inklużi l-kompletezza tar-Reġistru tar-Riskji u l-evidenza tat-trattamenti.

11. Standards u oqfsa ta' referenza

11.1 Din il-politika hija allinjata b'mod espliċitu mal-istandards u l-oqfsa li ġejjin sabiex jiġi żgurat li tissodisfa l-aħjar prattiki internazzjonali u l-aspettattivi regolatorji għall-ġestjoni tar-riskju tas-sigurtà tal-informazzjoni:

11.2 ISO/IEC 27001:

11.2.1 Klawżola 6.1: Tistabbilixxi r-rekwiżiti għall-identifikazzjoni tar-riskji u l-opportunitajiet, inkluż iċ-ċiklu sħiħ tal-ħajja tal-valutazzjonijiet u tat-trattamenti tar-riskju tas-sigurtà tal-informazzjoni. Din il-politika tagħmel operattivi l-Klawżoli 6.1.2 u 6.1.3 permezz ta' qafas strutturat li jobbliga identifikazzjoni, analiżi, valutazzjoni, trattament u protokolli dokumentati għall-aċċettazzjoni tar-riskju residwu.

11.2.2 Klawżola 8.32: L-integrazzjoni ta' ħsieb ibbażat fuq ir-riskju fil-proċessi tal-ġestjoni tat-tibdil tiżgura li l-bidliet organizzattivi sinifikanti kollha jwasslu għal rivalutazzjonijiet formali tar-riskju.

11.2.3 Klawżola 10: It-titjib kontinwu huwa integrat permezz ta' rieżamijiet regolari tal-politika, analiżi tax-xejriet tar-riskju u aġġornamenti tas-SoA mmexxija minn tagħlim miksub mir-riskju.

11.3 ISO/IEC 27005:

11.3.1 Tipprovdi gwida speċjalizzata u dettaljata dwar il-ġestjoni tar-riskju tas-sigurtà tal-informazzjoni. Din il-politika timplimenta l-mudell sħiħ tal-proċess tar-riskju ta' ISO/IEC 27005: Stabbiliment tal-Kuntest, Identifikazzjoni tar-Riskju, Analiżi tar-Riskju, Valutazzjoni tar-Riskju, Trattament tar-Riskju, Aċċettazzjoni tar-Riskju, Komunikazzjoni tar-Riskju, Monitoraġġ u Rieżami tar-Riskju.

11.4 ISO 31000:

11.4.1 Din il-politika tintegra l-prinċipji ta' ISO 31000 bħall-impenn tat-tmexxija, l-integrazzjoni mat-teħid tad-deċiżjonijiet u t-titjib kontinwu. Tiżgura li l-ġestjoni tar-riskju tkun integrata fil-kultura u fl-operazzjonijiet tal-organizzazzjoni.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Hija allinjata mal-gwida tan-NIST għat-twettiq ta' valutazzjonijiet tar-riskju, inklużi l-identifikazzjoni tat-theddid, l-analiżi tal-vulnerabbiltajiet, l-istima tal-probabbiltà u d-determinazzjoni tal-impatt. L-istruttura ta' din il-politika tirrifletti l-passi ddefiniti tan-NIST għall-valutazzjoni tar-riskju u tadattahom kemm għall-proċessi tekniċi kif ukoll għal dawk tan-negozju.

11.6 NIST SP 800-39:

11.6.1 Jappoġġa l-governanza tar-riskju fil-livell tal-intrapriża, b'enfasi fuq il-ġestjoni tar-riskju fuq livelli differenti fil-livelli organizzattivi, tal-missjoni/proċess tan-negozju u tas-sistema tal-informazzjoni. Din il-politika tiżgura li s-sjieda tar-riskju tkun definita b'mod ċar fil-livelli kollha u tinkludi strateġiji ta' trattament fil-livell organizzattiv.

11.7 GDPR tal-UE:

11.7.1 Artikolu 24: Jeħtieġ l-implimentazzjoni ta' miżuri tekniċi u organizzattivi xierqa biex jiġi żgurat li r-riskji għall-protezzjoni tad-data jiġu ġestiti kif suppost — indirizzati permezz tal-proċess strutturat tar-riskju ta' din il-politika.

11.7.2 Artikolu 25: "Protezzjoni tad-data mid-disinn u b'mod awtomatiku" hija allinjata mal-integrazzjoni tat-trattament tar-riskju fid-disinji tas-sistemi u tal-proċessi.

11.7.3 Artikolu 32: Jobbliga approċċ ibbażat fuq ir-riskju għall-miżuri tas-sigurtà — issodisfat permezz ta' valutazzjonijiet tar-riskju bbażati fuq l-impatt u l-għażla tal-kontrolli.

11.8 Direttiva NIS2 tal-UE:

11.8.1 Artikolu 21(2)(a–d): Jeħtieġ li l-entitajiet iwettqu valutazzjonijiet tar-riskju, jimplimentaw politiki dwar l-analiżi tar-riskju, u jiżguraw miżuri ta' sigurtà proporzjonati. Din il-politika tissodisfa dawn l-obbligi permezz tal-applikazzjoni kontinwa taċ-ċiklu tal-ħajja tar-riskju u ta' governanza dokumentata.

11.9 DORA tal-UE:

11.9.1 Artikolu 5: Jobbliga qafas dokumentat tal-ġestjoni tar-riskju tal-ICT — kopert b'mod sħiħ mill-arkitettura ta' din il-politika, inkluż l-immappjar tas-SoA u l-indikaturi ewlenin tar-riskju.

11.9.2 Artikolu 6: Jeħtieġ l-integrazzjoni tal-ġestjoni tar-riskju fi strateġiji ta' reżiljenza operattiva, indirizzata permezz ta' matriċijiet ta' eskalazzjoni u traċċar ta' assi kritiċi.

11.10 COBIT 2019:

11.10.1 APO12 – Ġestjoni tar-Riskju: Jikkorrispondi direttament mal-istabbiliment mill-organizzazzjoni ta' approċċ strutturat għall-ġestjoni tar-riskju, l-assenjazzjoni tar-rwoli, it-traċċar tat-trattamenti u l-iżgurar tar-responsabbiltà fil-livell tal-Bord.

11.10.2 MEA01 – Monitoraġġ, Valutazzjoni u Analiżi tal-Prestazzjoni u l-Konformità: Rifless fl-enfasi ta' din il-politika fuq l-analiżi tax-xejriet, il-monitoraġġ tal-indikaturi ewlenin tar-riskju, u l-integrazzjoni tal-feedback tal-awditjar fiċ-ċikli ta' titjib kontinwu.